IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellants:	Christopher J. Davenport	§ §	Confirmation No.:	7317
Serial No.:	10/773,973	§ §	Group Art Unit:	2135
Filed:	02/06/2004	§ §	Examiner:	T. B. Truong
For:	System And Method For Authentication Via A Single Sign-On Server	§ § §	Docket No.:	200315375-1

APPEAL BRIEF

Mail Stop Appeal Brief – Patents
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Date: January 28, 2008

Sir:

Appellants hereby submit this Appeal Brief in connection with the above-identified application. A Notice of Appeal was electronically filed on November 29, 2007.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real party in interest is the Hewlett-Packard Development Company (HPDC), a Texas Limited Partnership, having its principal place of business in Houston, Texas. HPDC is a wholly owned affiliate of Hewlett-Packard Company (HPC). The Assignment from the inventors to HPDC was recorded on February 6, 2004, at Reel/Frame 014975/0398.

II. RELATED APPEALS AND INTERFERENCES

Appellants are unaware of any related appeals or interferences.

III. STATUS OF THE CLAIMS

Originally filed claims:	1-24.
Claim cancellations:	12, 14, 15, 17 and 21.
Added claims:	None.
Presently pending claims:	1-11, 13, 16, 18-20 and 22-24.
Presently appealed claims:	1-11, 13, 16, 18-20 and 22-24.

IV. STATUS OF THE AMENDMENTS

No claims were amended after the final Office action dated November 1, 2007.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

The invention of claim 1 is directed to a system that comprises a client workstation,[1] a single sign-on ("SSO") server[2] accessible to the client workstation, and a plurality of host servers[3] accessible to the client workstation. A unique public key is associated with each host server.[4] Access by the client workstation to a first host server causes the client workstation to be automatically re-directed to the SSO server. The SSO server causes the client workstation to request sign-on credentials from a user if the user has not signed on to any of the host servers. The first host server, not the SSO server, then authenticates the user.[5] The sign-on credentials are used to authenticate the user upon accessing each host server.[6] Further, the sign-on credentials are encrypted with the public key associated with the host server for which the sign-on credentials were most recently used to authenticate the user.[7]

The invention of claim 9 is directed to a client workstation[8] configured to access any one or more of a plurality of services.[9] The client workstation comprises a CPU,[10] an input device[11] coupled to the CPU, and storage[12] coupled to the CPU. The storage contains a browser[13] that is executed by the CPU and that causes the workstation to browse to a service that runs in a host server, automatically re-direct to an SSO server, and permit the host server to

[1] Fig. 1, client workstation 51. P. 2, l. 2-4 of para. [0008].

[2] Fig. 1, SSO server 60. P. 2, l. 2-4 of para. [0008].

[3] Fig. 1, host servers 52-56. P. 2, l. 2-4 of para. [0008].

[4] P. 5, l 1 of para. [0016] through p. 6, l. 17 of para. [0018].

[5] Fig. 1. P. 4 l. 1 of para. [0013] through p. 6, l. 12 of para. [0017].

[6] P. 3-4, l. 1-12 of para. [0011].

[7] P. 5, l. 1-4 of para. [0016]; p. 6, l. 14-17 of para. [0018].

[8] Fig. 1, client workstation 51. P. 2, l. 2-4 of para. [0008].

[9] Fig. 1, services 53-57. P. 2, l. 4-6 of para. [0008].

[10] Fig. 2, CPU 80. P. 3, l. 3 of para. [0009].

[11] Fig. 2, input device 86. P. 3, l. 4 of para. [0009].

[12] Fig. 2, storage 82. P. 3, l. 4 of para. [0009].

[13] Fig. 2, browser 70. P. 3, l. 2 of para. [0010].

authenticate a user.[14] The authentication is either by requiring the user to enter credentials via the input device if the user has not already signed-on to a service and providing the credentials to the host server or, without the user entering credentials, by providing credentials previously stored in the storage to the host server if the user has already signed-on to a service and providing the credentials to the host server.[15] The credentials are encrypted using a public key associated with the host server that the client workstation most recently accessed.[16]

The invention of claim 13 is directed to an SSO server[17] that comprises a CPU[18] and storage. [19] The storage contains executable software[20] that causes the SSO server to cause user credentials to be entered by a user of a first computer if the user has not already signed-on to a service and to be encrypted using a first public key associated with a host computer, or to cause user credentials previously stored in the first computer to be retrieved, decrypted, and then encrypted using a second public key associated with a second computer. The first public key is different than the second public key. [21] The software also causes the user credentials to be used by the second computer to authenticate the user.[22]

The invention of claim 16 is directed to a host computer[23] on which a user accessible service[24] is executed. The host computer comprises a CPU[25] and

[14] P. 4, l. 1-10 of para. [0012].

[15] Fig. 1. P. 4 l. 1 of para. [0013] through p. 6, l. 12 of para. [0017].

[16] P. 5, l. 1-4 of para. [0016]; p. 6, l. 14-17 of para. [0018].

[17] Fig. 1, SSO server 60. P. 2, l. 2-4 of para. [0008].

[18] Fig. 2, CPU 80. P. 3, l. 3 of para. [0009].

[19] Fig. 2, storage 82. P. 3, l. 4 of para. [0009].

[20] Fig. 2, browser 70. P. 3, l. 2 of para. [0010].

[21] P. 5, l. 1-4 of para. [0016]; p. 6, l. 14-17 of para. [0018].

[22] P. 3-4, l. 1-12 of para. [0011].

[23] Fig. 1, host servers 52-56. P. 2, l. 2-4 of para. [0008].

[24] Fig. 1, services 53-57. P. 2, l. 4-6 of para. [0008].

[25] Fig. 2, CPU 80. P. 3, l. 3 of para. [0009].

executable software.[26] The software causes the CPU to cause a user's browser to be re-directed to a first computer to obtain user credentials and causes a user's browser to be re-directed back to the host computer so that the host computer can authenticate the user using the credentials.[27] Further, the software causes the CPU to decrypt the credentials using a private key associated with the host computer. [28]

The invention of claim 18 is directed to a system that comprises means[29] for providing user identifying information from a user if the user has not already signed-on to a service. The system also comprises means for retrieving[30] user identifying information previously stored in a computer if the user has already signed-on to a service and means for hosting a service and for authenticating the user using the user identifying information.[31] The system further includes means for encrypting user credentials using a public key associated with a means for hosting. [32] A different public key is associated with each of multiple means for hosting.

[26] Fig. 2, browser 70. P. 3, l. 2 of para. [0010].

[27] Fig. 1. P. 4 l. 1 of para. [0013] through p. 6, l. 12 of para. [0017].

[28] P. 5 l. 7-9 of para. [0015].

[29] Fig. 2, input device 86. P. 3, l. 4 of para. [0009].

[30] Fig. 1, SSO server 60. P. 2, l. 2-4 of para. [0008].

[31] Fig. 1, host servers 52-56. P. 2, l. 2-4 of para. [0008].

[32] Fig. 1, SSO server 60. P. 2, l. 2-4 of para. [0008].

The invention of claim 20 is directed to a method that comprises accessing a host server,[33] automatically re-directing from the host server to a sign-on server, and either retrieving previously stored user credentials if a user has already accessed a service or requesting the user to enter user credentials if the user has not already accessed a service.[34] The method further comprises re-directing back to the host server and the host server authenticating the user using the user credentials.[35] Further, the method comprises encrypting the user credentials with a public key associated with the host server that the user most recently accessed.[36] A different public key is associated with each of multiple host servers.[37]

[33] Fig. 1, host servers 52-56. P. 2, l. 2-4 of para. [0008].

[34] Fig. 1. P. 4 l. 1 of para. [0013] through p. 5, l. 2 of para. [0015].

[35] Fig. 1. P. 5 l. 4 of para. [0016] through p. 6, l. 12 of para. [0017].

[36] P. 5, l. 1-4 of para. [0016]; p. 6, l. 14-17 of para. [0018].

[37] P. 5, l. 1-4 of para. [0016]; p. 6, l. 14-17 of para. [0018].

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1, 9, 13, 18, and 20 comply with 35 U.S.C. § 112, second paragraph.

Whether claims 1-11, 13, 16, 18-20, and 22-24 are unpatentable over Biswas (U.S. Pat. No. 7,174,383) in view of Fang (U.S. Pat. No. 6,240,512).

VII. ARGUMENT

A. The § 112, second paragraph rejections

With regard to certain limitations in claims 1, 9, 13, 18, and 20, the Examiner alleged that such limitations are not "clearly explained anywhere in the specification" and that Appellants are required to point out where support in the specification can be found for such limitations. Final Office Action pp. 2-3. The Examiner, however, did not allege that the specific limitations on which the Examiner focused are not clear and understandable. Rather, the Examiner simply asked to be shown support in the specification. The Examiner's concerns seem to have nothing do with the claim clarify requirements of § 112, second paragraph. Accordingly, Appellants respectfully submit that the Examiner has not established a proper basis for a § 112, second paragraph, rejection.

At any rate, Appellants submit that the specification does support the limitations focused on by the Examiner. With regard to claim 1, the Examiner focused on the limitation "wherein said sign-on credentials are encrypted with the public key associated with the host server for which the sign-on credentials were most recently used to authenticate the user." With regard to claim 9, the Examiner focused on "said credentials are encrypted using a public key associated with the host server that the client workstation most recently accessed." These limitations are supported in the specification at least at pp. 5-7, paras. [0016]-[0018]. In para. [0016], an example is provided whereby the user attempts to access a service on server 52 and the credentials are encrypted using the public key of server 52. In para. [0018], the user then attempts to access a service on server host server 54. The credentials are encrypted using the public key of server 54. Appellants have described a single sign-on mechanism and has described using a public key associated with the most recently accessed server to encrypt the credentials. Thus, the limitations quoted above are supported by the specification.

With regard to claim 13, the Examiner focused on "decrypted, and then encrypted using a second public key associated with a second computer, the first public key being different than the second public key." This limitation is taught as explained above at paras. [0016]-[0018]. For example, para. [0018] states that the "SSO server 60 causes the credentials to be decrypted (if the credentials were stored in the cookie in encrypted form) and, if desired, causes the credentials to be encrypted using the public key associated with host server 54." Further, the specification explains that each host server has its own private key ("the host server 52 uses its own private key"—p. 6 para. [0017]). One of ordinary skill would understand that public keys are mathematically linked to private keys and thus that different private keys will have different public keys. Thus, if server 52 has its own private key, then there is a corresponding unique public key to server 52's private key.

With regard to claim 18 (similar issue for claim 20), the Examiner focused on there being a different public key for each means for hosting. Support for this limitation is provided above.

B. Overview of Biswas

Biswas is directed to single sign-on services. Biswas explains that, if a user attempts to sign on to a "partner application," the system redirects the request to a single sign-on server that requests the user to enter a credential. The single sign-on server verifies the user and issues the user a "token." The token grants the user access to other partner applications. Col. 1, l. 61 through col. 2, l. 11.

C. Overview of Fang

Fang is also directed to a single sign-on mechanism. Fang's system employs "master key synchronization." Fang teaches that a user's primary password can be used to encrypt all of the user's secondary passwords. Col. 1, ll. 45-47.

D. The obviousness rejections over Biswas in view of Fang

1. The Examiner's statements regarding Biswas are self-contradictory

Claim 1 requires that the sign-on credentials are encrypted with the public key associated with the host server for which the credentials were most recently used to authenticate the user. With regard to claim 1, the Examiner stated that "[a]lthough Biswas teaches wherein said sign-on credentials are encrypted with the public key associated with the host server for which the sign-on credentials were most recently used to authenticate the user, Biswas is silent on the capability of encrypting with the public key." Office Action p. 4. Similar statements were made with regard to claims 9, 13, 16 (regarding decryption) and 18. If the Examiner's statement is correct that Biswas is silent as to encrypting the credentials with the public key, then the Examiner's statement that "Biswas teaches wherein said sign-on credentials are encrypted with the public key associated with the host server for which the sign-on credentials were most recently used to authenticate the user" cannot be correct. The two statements would seem to be mutually exclusive.

2. The Examiner's obviousness rejections do not establish sufficient justification for combining Biswas and Fang

Regarding claim 1, the Examiner states that Fang teaches the limitation missing from Biswas. The Examiner then stated that it would have been obvious (a) to "have modified the invention of Biswas…with the teaching of Fang…by implementing a single-sign-on (SSO) mechanism that coordinates logons to local and remote resources…" and (b) to have modified the invention of Biswas…with the teaching of Fang to facilitate single-sign-on services in a hosting environment." Final Office Action p. 4. These statements are merely conclusions. The Examiner neglected to explain why it would have been obvious to combine Fang and Biswas. Absent even an attempt at justifying the combination, the Examiner's obviousness rejection of claim 1 is improper. See MPEP § 2143. This same defect is present in the Examiner's rejection of all claims.

3. Biswas and Fang lack at least one claim limitation

Claim 1 requires "wherein said sign-on credentials are used to authenticate the user upon accessing each host server, and wherein said sign-on credentials are encrypted with the public key associated with the host server for which the sign-on credentials were most recently used to authenticate the user." The observations noted above regarding the self-contradictory nature of the

Examiner's analysis aside, the Examiner seems to believe that Biswas teaches encrypting user credentials using a public key associated with a host server, which according to claim 1, is the server accessible to the client workstation. The Examiner evidently believes that in Biswas the application servers 114-118 are akin to the claimed "host server." That being the case, then Biswas would have to teach that a public key associated with an application server 114-118 is used to encrypt the user credentials. Biswas, however, does not teach this feature. Instead, Biswas teaches that the user computer 102 includes a cryptographic module 204 that "can be used to encrypt user authentication credentials while these credentials are in transit across network 110." Col. 4, ll. 25-29. Biswas does not specify how the encryption works and certainly does not explain that a public key associated with any of the application servers 114-118 is used by the user computer 102. While Fang teaches a primary password being used to encrypt secondary passwords, Fang does not teach the limitation quoted above, in particular "wherein said sign-on credentials are encrypted with the public key associated with the host server for which the sign-on credentials were most recently used to authenticate the user" which the Examiner finds missing from Biswas. The Examiner also focused on a section of col. 10 in Fang, but that passage does not teach the specific limitation quoted above.

For at least this reason, the Examiner erred in rejecting claim 1 and all claims dependent thereon. This same reasoning applies also to claims 9 and 20 as well as claims dependent thereon.

Claim 13 requires that user credentials are encrypted using public keys associated with the host and second computers. Biswas lacks any such teaching as the Examiner seems to have conceded and as explained above. As previously established, Fang is also deficient in this regard.

Claim 16 requires that the host computer's CPU "decrypts the credentials using a private key associated with the host computer." Appellants find mention in Biswas of using a private key associated with a host computer to decrypt credentials, and the Examiner seems to concede as much. The Examiner believes the teaching missing from Biswas is found in Fang at col. 1, ll. 50-55 and col. 10, ll. 10-14. The passage from col. 1 is directed to verifying the primary password and then obtaining the secondary passwords by decrypting the encrypted passwords with the primary password. The primary password is not described as being a "private key associated with the host computer." The passage from col. 10 does not teach the limitation quoted above. For at least this reason, the Examiner erred in rejecting claim 16 and its dependent claims.

Claim 18 requires "means for encrypting user credentials using a public key associated with a means for hosting, a different public key being associated with each of multiple means for hosting." Biswas does not teach, as explained above, using a public key associated with an application server 114-118 to encrypt user credentials. Fang does not satisfy this deficiency. For at least this reason, the Examiner erred in rejecting claim 18 and its dependent claims.

E. Conclusion

For the reasons stated above, Appellants respectfully submit that the Examiner erred in rejecting all pending claims. It is believed that no extensions of time or fees are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. § 1.136(a), and any fees required (including fees for net addition of claims) are hereby authorized to be charged to Hewlett-Packard Development Company's Deposit Account No. 08-2025.

Respectfully submitted,

/Jonathan M. Harris/
Jonathan M. Harris, Reg. No. 44,144
CONLEY ROSE, P.C.
(713) 238-8000 (Phone)
(713) 238-8008 (Fax)
ATTORNEY FOR APPELLANTS

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
Legal Dept., M/S 35
P.O. Box 272400
Fort Collins, CO 80527-2400

VIII. CLAIMS APPENDIX

1. (Previously presented) A system, comprising:

a client workstation;

a single sign-on ("SSO") server accessible to the client workstation;

a plurality of host servers accessible to the client workstation, a unique public key being associated with each host server;

wherein access by the client workstation to a first host server causes the client workstation to be automatically re-directed to the SSO server and the SSO server causes the client workstation to request sign-on credentials from a user if the user has not signed on to any of the host servers, and wherein the first host server, not the SSO server, authenticates the user; and

wherein said sign-on credentials are used to authenticate the user upon accessing each host server, and wherein said sign-on credentials are encrypted with the public key associated with the host server for which the sign-on credentials were most recently used to authenticate the user.

2. (Previously presented) The system of claim 1 wherein, upon being re-directed to the SSO server, the first host server supplies the SSO server with security information that is used to encrypt sign-on credentials.

3. (Previously presented) The system of claim 1 wherein the user's sign-on credentials are stored in the client workstation.

4. (Previously presented) The system of claim 1 wherein the user's sign-on credentials are stored in the SSO server.

5. (Previously presented) The system of claim 3 wherein, after the first host server authenticates the user, the client workstation accesses a second host server which causes the client workstation to be automatically re-directed to the

SSO server, and wherein the SSO server causes the sign-on credentials to be retrieved and used by the second host server to authenticate the user without the user supplying additional sign-on credentials.

6. (Previously presented) The system of claim 1 wherein the user's sign-on credentials are stored in a cookie in the client workstation.

7. (Previously presented) The system of claim 1 wherein the user's sign-on credentials are stored in encrypted form in a cookie in the client workstation.

8. (Previously presented) The system of claim 1 wherein, after requesting sign-on credentials from the user, the client workstation is automatically re-directed back to the first host server to authenticate the user.

9. (Previously presented) A client workstation configured to access any one or more of a plurality of services, comprising:

a CPU;

an input device coupled to the CPU; and

storage coupled to the CPU, said storage containing a browser that is executed by the CPU and that causes the workstation to:

browse to a service that runs in a host server;

automatically re-direct to a single sign-on ("SSO") server; and

permit the host server to authenticate a user either by requiring the user to enter credentials via the input device if the user has not already signed-on to a service and providing the credentials to the host server or, without the user entering credentials, by providing credentials previously stored in the storage to the host server if the user has already signed-on to a service and providing the credentials to the host server;

wherein said credentials are encrypted using a public key associated with the host server that the client workstation most recently accessed.

10. (Original) The client workstation of claim 9 wherein the CPU further causes the workstation to be re-directed back to the service to permit the host server to authenticate the user.

11. (Previously presented) The client workstation of claim 9 wherein the credentials are stored in the storage.

12. (Canceled).

13. (Previously presented) A single sign-on ("SSO") server, comprising:

a CPU;

storage coupled to the CPU, said storage containing software that is executed by the CPU and that causes the SSO server to:

cause user credentials to be entered by a user of a first computer if the user has not already signed-on to a service and to be encrypted using a first public key associated with a host computer, or to cause user credentials previously stored in the first computer to be retrieved, decrypted, and then encrypted using a second public key associated with a second computer, the first public key being different than the second public key; and

cause the user credentials to be used by the second computer to authenticate the user.

14. (Canceled).

15. (Canceled).

16. (Previously presented) A host computer on which a user accessible service is executed, comprising:

a CPU; and

software executable by said CPU;

wherein the CPU causes a user's browser to be re-directed to a first computer to obtain user credentials and that causes a user's browser to be re-directed back to the host computer so that the host computer can authenticate the user using the credentials;

wherein the CPU decrypts the credentials using a private key associated with the host computer.

17. (Canceled).

18. (Previously presented) A system, comprising:

means for providing user identifying information from a user if the user has not already signed-on to a service;

means for retrieving user identifying information previously stored in a computer if the user has already signed-on to a service;

means for hosting a service and for authenticating the user using the user identifying information; and

means for encrypting user credentials using a public key associated with a means for hosting, a different public key being associated with each of multiple means for hosting.

19. (Original) The system of claim 18 further comprising means for generating a cookie that contains the user identifying information and for storing the cookie in a user-controlled computer.

20. (Previously presented) A method, comprising:

accessing a host server;

automatically re-directing from the host server to a sign-on server;

either retrieving previously stored user credentials if a user has already accessed a service or requesting the user to enter user credentials if the user has not already accessed a service;

re-directing back to the host server; and

the host server authenticating the user using the user credentials; and

encrypting said user credentials with a public key associated with the host server that the user most recently accessed, a different public key being associated with each of multiple host servers.

21. (Canceled).

22. (Original) The method of claim 20 further comprising storing user-entered user credentials in a computer that is controllable by the user and that is not the sign-on server.

23. (Original) The method of claim 22 wherein storing the user credentials comprises storing the user credentials in a cookie that is stored in the computer.

24. (Original) The method of claim 20 further comprising, upon re-directing to the sign-on server, determining whether the user has already accessed a service.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.